



CVE-2020-35659

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-35659
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-24 16:15:00 UTC
Updated	2020-12-28 17:40:00 UTC
Description	The DNS query log in Pi-hole before 5.2.2 is vulnerable to stored XSS. An attacker with the ability to directly or indirectly qu

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pi-hole	Pi-hole	All	All	All	All
Application	Pi-hole	Pi-hole	All	All	All	All

References

Reference

- [Pi-hole Patches Critical Stored XSS Vulnerability – Rich Mirch](#)
- [Pi-hole Core/Web v5.2.2 and FTL v5.3.4 released! - Announcements - Pi-hole Userspace](#)
- [Prevent malformed DNS queries executing JS on querylog/long term query pages by PromoFaux · Pull Request #1665 · pi-hole/AdminLTE · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)